



CÓMO PROTEGER SU RED INALÁMBRICA

Cada vez más son más los usuarios de computadoras que se interesan en la conveniencia y movilidad que brinda el acceso inalámbrico a Internet. Actualmente, las personas que viajan por negocios usan computadoras portátiles para mantenerse en contacto con sus oficinas; los turistas mandan fotos a sus amigos desde sus lugares de vacaciones y los compradores hacen sus pedidos cómodamente sentados en el sofá de sus casas. Una red inalámbrica (*wireless network*) puede conectar varias computadoras ubicadas en distintas partes de su casa o negocio sin enredos de cables y le permite trabajar en una computadora portátil desde cualquier lugar dentro del área de la red.

Generalmente, para acceder a Internet sin cables es necesario tener instalada una conexión de banda ancha, esto se llama “punto de acceso” (*access point*), como por ejemplo una línea de cable o DSL que funciona conectada a un módem. Para instalar la red inalámbrica, usted conecta el punto de acceso a un enrutador inalámbrico (*wireless router*) que emite una señal al aire que en algunas oportunidades tiene un radio de emisión de hasta varios cientos de pies. Cualquier computadora que esté equipada con una tarjeta de cliente inalámbrico (*wireless client card*) que se encuentre dentro del radio de emisión del enrutador puede captar la señal del aire y acceder a Internet.

El aspecto negativo de una red inalámbrica es que, a menos que usted tome ciertas precauciones, cualquier usuario que tenga una computadora preparada para acceder a Internet sin cable puede usar su red. Esto significa que sus vecinos, o en el peor de los casos los ciber-delincuentes o *hackers* que andan al acecho cerca de su computadora, podrían “colgarse” de su red, o hasta podrían lograr acceder a la información almacenada en su computadora. Si una persona no autorizada usa su red para cometer un delito o enviar mensajes electrónicos *spam*, la actividad puede ser rastreada hasta su cuenta de usuario.

Afortunadamente, hay algunos pasos que usted puede seguir para proteger su red inalámbrica y las computadoras conectadas a la misma.

Pasos Preventivos

1. Use encriptación. La manera más efectiva de proteger su red inalámbrica contra los intrusos es encriptar o codificar las comunicaciones en red. La mayoría de los enrutadores inalámbricos, puntos de acceso y estaciones base tienen un mecanismo de encriptación incorporado. Si su enrutador inalámbrico no tiene esta función de encriptación, considere conseguir uno que sí la tenga.

Los fabricantes de enrutadores inalámbricos frecuentemente despachan sus aparatos con la función de encriptación desactivada y usted debe activarla. En el manual de instrucciones de su enrutador inalámbrico debería encontrar la descripción del procedimiento para instalarla. Si no fuera así, consulte el sitio Web del fabricante del enrutador.



CÓMO PROTEGER SU RED INALÁMBRICA

Hay dos tipos principales de encriptación: Acceso Protegido para Transferencia Inalámbrica de Datos o **WPA** (por su acrónimo del inglés *Wi-Fi Protected Access*) y Equivalencia de Privacidad Inalámbrica o **WEP** (por su acrónimo del inglés *Wired Equivalent Privacy*). Su computadora, enrutador y demás equipo deben utilizar la misma encriptación. El sistema WPA provee una encriptación más potente; si tiene la opción, use este sistema ya que está diseñado para protegerlo contra la mayoría de los ataques de los *hackers*.

Algunos modelos más antiguos de enrutadores solamente ofrecen encriptación WEP, lo que es mejor que no tener ningún tipo de encriptación. Este sistema de encriptación o codificación debería proteger su red inalámbrica contra las intrusiones accidentales de vecinos o contra los ataques de *hackers* menos sofisticados. Si usa el sistema de encriptación WEP, configúrelo al nivel de seguridad más alto.

2. Use software antivirus y *anti-spyware* y también active el *firewall*. Las computadoras conectadas a una red inalámbrica necesitan tener la misma protección que las computadoras conectadas al Internet por medio de un cable. Instale en su computadora un software antivirus y *anti-spyware* y manténgalos actualizados. Si su computadora fue entregada con el *firewall* o cortafuegos desactivado, actívelo.

3. Desactive el identificador de emisión. Casi todos los enrutadores inalámbricos (*wireless routers*) tienen un mecanismo llamado identificador de emisión (*identifier broadcasting*). Este mecanismo emite una señal a todas las terminales que estén en las cercanías anunciando su presencia. No es necesario que usted emita esta información si la persona que está usando la red ya sabe que está disponible. Los *hackers* pueden usar el identificador de emisión para acceder a redes inalámbricas vulnerables. Si su enrutador inalámbrico se lo permite, desactive el mecanismo del identificador de emisión.

4. Cambie la configuración predeterminada del identificador de su enrutador (*router's pre-set password for administration*). Probablemente, el identificador de su enrutador sea un código o nombre de identificación (ID) estándar predeterminado que fue asignado por el fabricante para todas las unidades de hardware de ese modelo. Aunque su enrutador no esté emitiendo la señal de su identificador a todo el mundo, los *hackers* conocen los códigos o nombres de identificación predeterminados y pueden usarlos para intentar acceder a su red. Cambie el identificador de su enrutador por un código que solamente usted conozca, y recuerde que para que su enrutador y su computadora puedan comunicarse entre sí, debe configurar el mismo código de identificación o ID en ambos. Use una contraseña que tenga por lo menos 10 caracteres: Cuanto más extensa sea su contraseña o código de identificación, más difícil resultará que los *hackers* logren acceder a su red.



CÓMO PROTEGER SU RED INALÁMBRICA

5. Cambie la contraseña predeterminada de instalación del enrutador. Probablemente, el fabricante de su enrutador inalámbrico le asignó una contraseña estándar predeterminada para permitir la instalación y operación del enrutador (*pre-set password for administration*). Los *hackers* conocen estas contraseñas predeterminadas, por lo tanto, cámbiela por una contraseña nueva y que solamente usted conozca. Cuanto más extensa sea la contraseña, más difícil será descifrarla.

6. Solamente permita el acceso a su red inalámbrica a computadoras específicas. Cada computadora habilitada para comunicarse con una red tiene asignada una dirección exclusiva de Control de Acceso a Medios o MAC (por su acrónimo del inglés, *Media Access Control*). Generalmente, los enrutadores inalámbricos tienen un mecanismo que permite que solamente los aparatos con una dirección MAC particular puedan acceder a la red. Algunos *hackers* han imitado domicilios MAC, por lo tanto no se confíe solamente en esta medida de protección.

7. Apague su red inalámbrica cuando sepa que no la va a utilizar. Los *hackers* no pueden acceder a un enrutador inalámbrico cuando está apagado. Si usted apaga el enrutador cuando no lo usa, está limitando la cantidad de tiempo de vulnerabilidad a los ataques de los *hackers*.

8. No dé por supuesto que los “hot spots” públicos son seguros. Muchos bares, hoteles, aeropuertos y otros establecimientos públicos ofrecen redes inalámbricas para sus clientes. Estos “hot spots” o puntos de acceso a Internet son convenientes, pero no siempre son seguros. Consulte con el propietario del establecimiento para verificar cuáles son las medidas de seguridad implementadas.

Tenga cuidado con el tipo de información a la que accede o que envía desde una red inalámbrica pública. Para evitar riesgos, debería tener en cuenta que otras personas pueden acceder a cualquier información que usted vea o envíe a través de una red inalámbrica pública. A menos que usted pueda verificar que un “hot spot” haya implementado medidas de seguridad efectivas, lo mejor es evitar el envío o recepción de información delicada a través de la red.

Pruebe su conocimiento de estos y otros consejos en www.AlertaenLinea.gov/prueba.

Glosario

Acceso Protegido para Transferencia Inalámbrica de Datos - WPA (*Wi-Fi Protected Access*): Protocolo de seguridad desarrollado para reparar defectos del protocolo WEP. Encripta o codifica los datos transferidos desde y hacia los dispositivos inalámbricos conectados dentro de una red.

Dirección de Control de Acceso a Medios - MAC (*Media Access Control Address*): Número exclusivo asignado por el fabricante a cada computadora u otro dispositivo de una red.



CÓMO PROTEGER SU RED INALÁMBRICA

Encriptación – Codificación (*Encryption*): Codificación de los datos en un código secreto que solamente puede ser decodificado o leído por el software instalado para decodificar la información.

Equivalencia de Privacidad Inalámbrica - WEP (*Wired Equivalent Privacy*): Protocolo de seguridad que encripta o codifica los datos transferidos desde y hacia los dispositivos inalámbricos conectados dentro de una red. No provee tanta seguridad como una encriptación WPA.

Enrutador - Encaminador - Interfaz (*Router*): Dispositivo que conecta dos o más redes. Un enrutador encuentra la mejor vía para transferir la información a través de las redes.

Firewall o Cortafuegos: Programa hardware o software diseñado para impedir que los *hackers* usen su computadora para enviar información personal sin su autorización. Los programas *firewall* vigilan los intentos exteriores de acceder a su sistema y bloquean las comunicaciones de y hacia fuentes no autorizadas por el usuario.

Identificador de Servicios Ampliables - ESSID (*Extended Service Set Identifier*): Nombre o código asignado por el fabricante a un enrutador. Puede ser un nombre o código estándar predeterminado asignado por el fabricante a todas las unidades de hardware de ese modelo. Los usuarios pueden optimizar la seguridad cambiándolo a un nombre exclusivo. Similar a un Identificador de Conjunto de Servicio o *Service Set Identifier* (SSID).

Punto de Acceso Público a Internet (*Hot Spot*): Lugares públicos (bares, hoteles, aeropuertos, etc.) que ofrecen acceso inalámbrico a sus clientes.

Red Inalámbrica (*Wireless Network*): Sistema de red que conecta computadoras entre sí o al Internet sin conexión de cables.

Transferencia Inalámbrica de Datos (*Wi-Fi*): Tecnología inalámbrica para acceder a Internet o para conectar computadoras entre sí.

Alerta en Línea ofrece recomendaciones prácticas brindadas por el gobierno federal y la industria tecnológica para ayudarlo a protegerse contra el fraude en el Internet, mantener su computadora segura y proteger su información personal.

Mayo 2006